ESET **ENDPOINT SECURITY para ANDROID**

Guia do Usuário

(destinado ao produto versão 2.0 e posterior)

Clique aqui para fazer download da versão mais recente deste documento

ESET **ENDPOINT SECURITY**

Atendimento ao cliente: www.eset.com/support

REV. 28. 8. 2015

Índice

1. Introdução

A nova geração de ESET Endpoint Security para Android (EESA) é feita para trabalhar com o ESET Remote Administrator (ERA) 6, o novo console de gerenciamento que permite o gerenciamento remoto de todas as soluções de segurança ESET. O ESET Endpoint Security para Android 2 é compatível apenas com o ERA 6 e versões posteriores.

O ESET Endpoint Security para Android é projetado para proteger dispositivos móveis corporativos contra as mais recentes ameaças de malware e proteger seus dados, mesmo se o dispositivo for perdido ou roubado. Isso também ajuda os administradores do sistema manterem seus dispositivos de acordo com as políticas de segurança da empresa.

O ESET Endpoint Security também pode ser aplicado em empresas pequenas e médias sem a necessidade de gerenciamento remoto via ESET Remote Administrator. Técnico de TI, administrador do sistema ou usuário real do Endpointpodem simplesmente compartilhar suas configurações do ESET Endpoint Security com outros colegas. Esse processo diminui completamente a necessidade de ativação do produto e de configuração manual de cada módulo do produto que pode ser exigido de outra forma logo depois da instalação do ESET Endpoint Security.

1.1 Novidades da versão 2

Controle de aplicativos

O Controle de aplicativos permite que os administradores monitorem os aplicativos instalados, bloqueiem o acesso a aplicativos definidos e diminuam o risco de exposição ao avisar os usuários para que desinstalem certos aplicativos. Consulte a seção Controle de aplicativos deste guia para obter mais informações.

Segurança do dispositivo

A segurança do dispositivo permite que os administradores executem políticas de segurança básicas em vários dispositivos móveis. Por exemplo, o administrador pode:

- definir o nível mínimo de segurança e complexidade de códigos de bloqueio de tela
- define o número máximo de tentativas falhas de desbloquear
- definir o tempo depois do qual os usuários devem alterar seu código de bloqueio de tela
- configurar o temporizador da tela de bloqueio
- restringir uso de câmera

Consulte a seção Segurança do dispositivo deste guia para obter mais informações.

Importar e exportar configurações

Para compartilhar facilmente as configurações de um dispositivo móvel com outro se o dispositivo não for gerenciado pelo ERA, o ESET Endpoint Security 2 apresenta a opção de exportar e importar configurações do programa. O administrador pode exportar manualmente configurações do dispositivo para um arquivo que pode então ser compartilhado (por exemplo, via email) e importado para qualquer dispositivo executando o aplicativo do cliente. Quando o usuário aceita o arquivo de configurações recebido, ele define automaticamente todas as configurações e ativa o aplicativo (desde que as informações de licença tenham sido incluídas). Todas as configurações são protegidas por uma senha de administrador.

Antiphishing

Esse recurso protege os usuários contra acessar sites maliciosos ao usar navegadores compatíveis (navegador padrão do Android e Chrome).

A tecnologia Anti-Phishing protege os usuários de tentativas de adquirir senhas, dados bancários e outras informações sensíveis em sites ilegítimos que se passam por sites legítimos. Quando um dispositivo tenta acessar um URL, o ESET Anti-Phishing compara o URL com o banco de dados do ESET de sites de phishing conhecidos. Se for encontrada uma correspondência, a conexão com o URL é abortada e uma mensagem de aviso é exibida.

Centro de notificação

O ESET Endpoint Security fornece aos usuários um centro de notificações unificado, onde eles podem encontrar todas as notificações em relação aos recursos do aplicativo que exigem sua atenção. O centro de notificações fornecerá informações sobre vários eventos, motivos pelos quais eles não estão em conformidade com as políticas da empresa e o que deve ser feito para cumprir esses requisitos. As notificações são organizadas de acordo com a prioridade, com notificações de maior prioridade mostradas no topo da lista.

Novo sistema de licenciamento

O ESET Endpoint Security é totalmente compatível com o ESET License Administrator - novo modelo de licenciamento introduzido com o ESET Remote Administrator 6.

Uma nova estrutura de licenciamento simplifica a implantação e uso a longo prazo do software de segurança ESET. Quando o cliente solicita uma alteração em sua licença, a alteração é refletida de forma automática e transparente em todos os produtos que usam a licença. Isso permite que os clientes usem seu endereço de email e uma senha personalizada como credenciais, em vez do nome de usuário e senha emitidos pela ESET usados por produtos mais antigos.

A introdução de chaves de licença e atualizações automáticas de licenças (mediante renovação ou qualquer outra operação de licença) significa que os clientes podem ter certeza de que estão protegidos. O portal do ESET License Administrator e a capacidade de atribuir direitos de autorização de licença por email (com base em informações de conta dos clientes) simplificam o gerenciamento e implantação de licenças. Usando o ESET License Administrator, os proprietários de licença podem delegar o gerenciamento de licenças a uma entidade responsável (mesmo um terceiro) sem perder o controle da licença.

Atualização gerenciada de um produto para uma compilação mais recente

Administradores de sistemas que usam o ERA e não desejam atualizar o ESET Endpoint Security para Android para a versão mais recente assim que ela se tornar disponível tem a opção de controlar o mecanismo de atualização.

Assistentes de instalação

O ESET Endpoint Security oferece o assistente de configuração pós-instalação para recursos selecionados, para tornar o processo mais simples.

Antivírus aprimorado

- Tempos do rastreamento em tempo real (no acesso) aprimorados
- Integrado ESET Live Grid
- 2 níveis de rastreamento - Inteligente e profundo
- Aprimoramentos de rastreamento sob demanda - rastreamento em segundo plano, pausa no rastreamento
- Rastreamento agendado - um rastreamento completo do dispositivo pode ser agendado pelo administrador
- Rastreamento no carregador - um rastreamento será iniciado automaticamente quando o dispositivo estiver no estado ocioso (totalmente carregado e conectado a um carregador)
- Configuração de atualização do banco de dados de vírus aprimorado - o administrador pode especificar o tempo de atualizações regulares e selecionar o servidor de atualização que os dispositivos usam (servidor de lançamento, servidor de pré-lançamento, imagem local)

Relatórios detalhados com resultados do rastreamento são enviados para o ERA. O ESET Endpoint Security inclui recursos da ESET Endpoint Security versão 1, como a detecção de aplicativos potencialmente inseguros, detecção de aplicativos potencialmente indesejados e USSD Control.

Filtro de SMS & Chamada aprimorado

SMS e Filtro de Chamadas, anteriormente conhecido como Antispam, protege os usuários contra chamadas, mensagens SMS e MMS indesejados. Esse recurso oferece agora dois tipos de regras: regras do administrador e regras do usuário, onde as regras do administrador são sempre superiores.

Outras melhorias incluem:

- Bloqueio com base no tempo - o usuário ou administrador pode bloquear chamadas e mensagens recebidas durante horários especificados
- Bloqueio com um toque para o remetente da última chamada ou mensagem, número de telefone, grupo de contatos, números desconhecidos ou ocultos

Antifurto aprimorado

Recursos Antifurto permitem que o administrador proteja e localize um dispositivo que esteja perdido ou roubado. As medidas do Antifurto podem ser acionadas a partir do ERA, ou através de comandos remotos.

O ESET Endpoint Security 2 usa os mesmos comandos remotos da versão 1 (Bloquear, Limpar e Encontrar). Os comandos a seguir, completamente novos, foram adicionados:

- **Desbloquear**-desbloqueia o aplicativo bloqueado
- **Redefinição de fábrica melhorada** - Todos os dados acessíveis no dispositivo serão removidos rapidamente (cabeçalhos de arquivos serão destruídos) e o dispositivo será redefinido para suas configurações padrão de fábrica.
- **Alarme** -o dispositivo perdido será bloqueado e reproduzirá um som muito alto mesmo se o dispositivo estiver no silencioso

Para fortalecer a segurança de comandos remotos, o administrador receberá um código de verificação SMS único e com tempo limitado em seu celular (no número definido na lista de contatos do Administrador) quando executar um comando remoto. Este código de verificação será usado para verificar um comando em particular.

Comandos Antifurto do ERA

Os comandos do Antifurto agora podem ser realizados também a partir do ERA. A nova funcionalidade de gerenciamento de dispositivos móveis permite que o administrador envie comandos Antifurto com apenas alguns cliques. As tarefas são imediatamente enviadas para execução através do componente do Conector de dispositivo móvel, que agora é uma parte da infraestrutura do ERA.

Contatos do administrador

Esta é a lista de números de telefone do administrador protegidos pela senha do administrador. Comandos Antifurto só podem ser enviados de números confiáveis.

Exibição de mensagem do ERA

Ao gerenciar dispositivos remotamente, o administrador pode enviar uma mensagem personalizada para um dispositivo em particular ou para um grupo de dispositivos. Isso ajuda a comunicar uma mensagem urgente para os usuários de dispositivos gerenciados. A mensagem será exibida na forma de um pop-up, para que o usuário não deixe de vê-la.

Informações personalizadas da tela de bloqueio

O administrador pode definir informações personalizadas (nome da empresa, endereço de email, mensagem) que serão exibidas quando o dispositivo for bloqueado, com a opção de ligar para um dos contatos do administrador pré-definidos.

Gerenciamento remoto aprimorado com o ESET Remote Administrator 6

Agora é possível configurar e definir todas as configurações do aplicativo através da política remota, a partir das configurações de Antivírus, SMS e Filtro de Chamadas e Segurança do dispositivo para restrições de controle de aplicativos, etc. Isso permite que os administradores apliquem a política de segurança da empresa em toda a rede, inclusive em dispositivos móveis.

O ESET Endpoint Security para Android versão 2 oferece um relatório muito melhor visível do console da Web ERA. Isto permite que os administradores identifiquem prontamente os dispositivos problemáticos e encontrem a origem do problema.

O gerenciamento de dispositivos Android agora é parte integrante do ESET Remote Administrator 6 com quase todas as mesmas funções disponíveis para os produtos desktop ESET, como o ESET Endpoint Antivirus 6 e o ESET Endpoint Security 6.

Administração local

O ESET Endpoint Security para Android oferece aos administradores a opção de configurar e gerenciar endpoints localmente, se eles optarem por não usar o ESET Remote Administrator. Todas as configurações do aplicativo são protegidas pela senha do administrador para que o aplicativo esteja totalmente sob controle em todos os momentos.

Distribuição e instalação do produto aprimorada

Além dos métodos de instalação tradicionais (fazer download e instalar um pacote a partir do site da ESET, distribuir o pacote de instalação via email), os administradores e usuários têm a opção de baixar e instalar o aplicativo a partir da loja do Google Play.

Ativação do produto aprimorada

Depois do download e instalação, o administrador ou usuário tem várias opções para ativar o produto:

- Eles podem usar as novas opções de licenciamento e inserir manualmente a chave de licença ou a conta do administrador de segurança.
- Eles podem clicar no link enviado em um email do administrador. O produto irá configurar a conexão ERA automaticamente e informações sobre a licença serão enviadas para o dispositivo a partir do ERA.
- O administrador pode inserir manualmente as informações de conexão ERA.
- Importar o arquivo que contém as configurações do aplicativo (com as informações da licença incluídas) vai ativar posteriormente o aplicativo.

Identificação aprimorada do dispositivo móvel no ERA

Durante o processo de inscrição, os dispositivos Android estão na lista de permissões, de forma que somente os dispositivos autorizados podem se conectar ao ERA. Isso melhora a segurança e também simplifica a identificação individual de dispositivos - cada dispositivo móvel é identificado por seu nome, descrição e IMEI. Dispositivos com apenas Wi-Fi são identificados pelo seu endereço MAC Wi-Fi.

Interface gráfica do usuário com novo design

O ESET Endpoint Security proporciona uma experiência de usuário aprimorada semelhante à experiência em destaque em todas as soluções ESET para clientes empresariais.

Facilidade de uso

Graças à nova interface de usuário, é mais fácil navegar e usar o produto. A estrutura da interface gráfica do usuário corresponde à nova geração de soluções ESET Endpoint e ao ESET Remote Administrator.

1.2 Requisitos mínimos do sistema

Para instalar o ESET Endpoint Security, seu dispositivo Android deve atender aos requisitos mínimos do sistema a seguir:

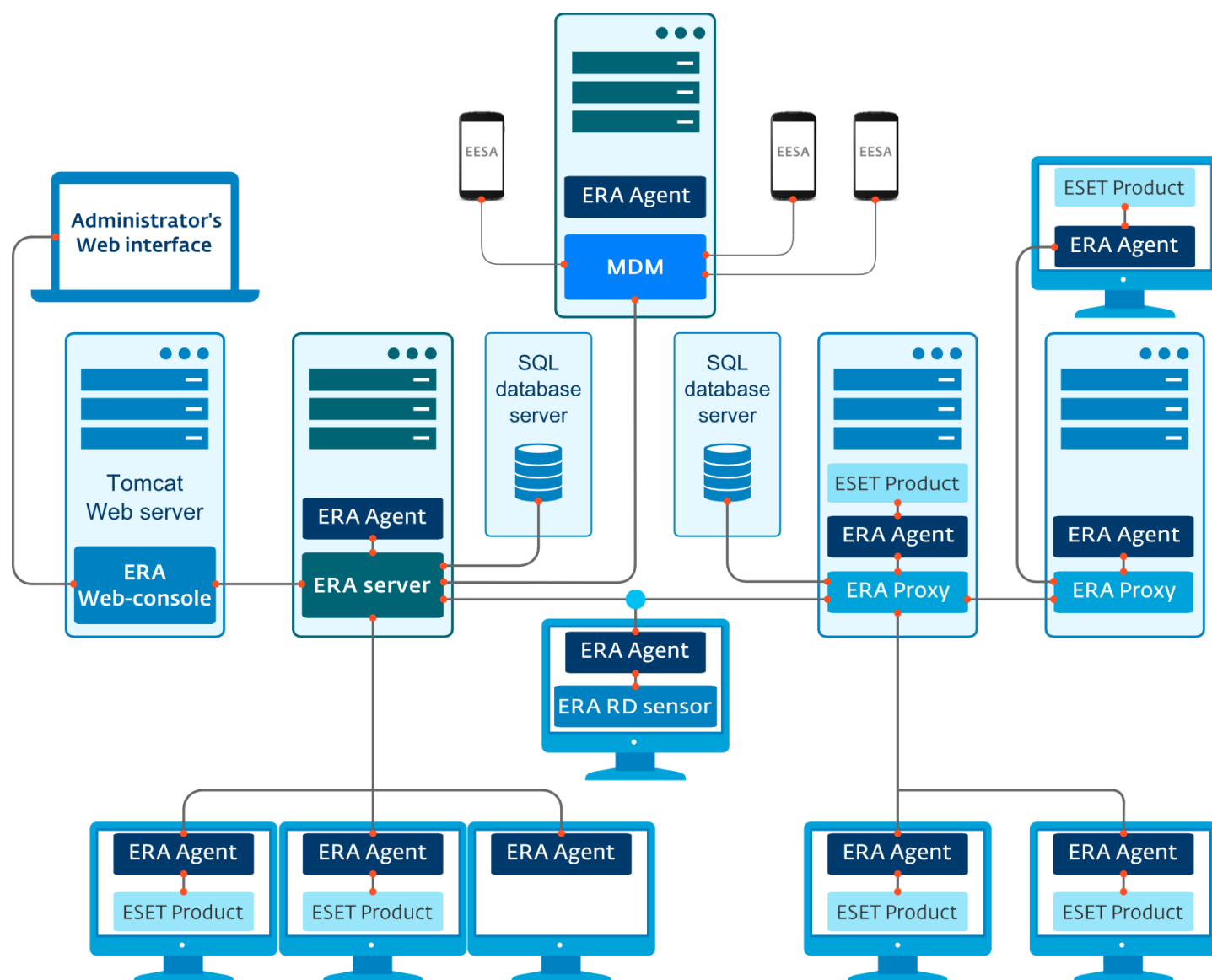
- Sistema operacional: Android 4 (Ice Cream Sandwich) e versões posteriores
- Resolução da tela de toque: 480x800 px
- CPU: ARM com conjunto de instrução ARMv7, x86 Intel Atom
- Espaço de armazenamento livre: 20 MB
- Conexão com a Internet

OBSERVAÇÃO: Dispositivos com SIM duplo e root não são compatíveis. Alguns recursos (por exemplo Antifurto e SMS e Filtro de Chamadas) não estão disponíveis em tablets que não suportam chamadas e mensagens.

2. Usuários conectados ao ESET Remote Administrator

ESET Remote Administrator (ERA) 6 é um aplicativo que permite que você gerencie produtos ESET em um ambiente em rede a partir de um local central. O sistema de gerenciamento de tarefas do ESET Remote Administrator permite que você instale soluções de segurança da ESET em computadores remotos e dispositivos móveis e responda rapidamente a novos problemas e ameaças. O ESET Remote Administrator não fornece proteção contra código malicioso por si só, ele conta com a presença de uma solução de segurança da ESET em cada cliente.

As soluções de segurança da ESET são compatíveis com redes que incluem vários tipos de plataforma. Sua rede pode incluir uma combinação de sistemas operacionais Microsoft, Linux e OS X que são executados em dispositivos móveis (celulares e tablets).

A imagem a seguir mostra uma arquitetura de exemplo para uma rede protegida por soluções de segurança da ESET gerenciada por ERA:

OBSERVAÇÃO: Para mais informações consulte a ESET Remote Administrator documentação online.

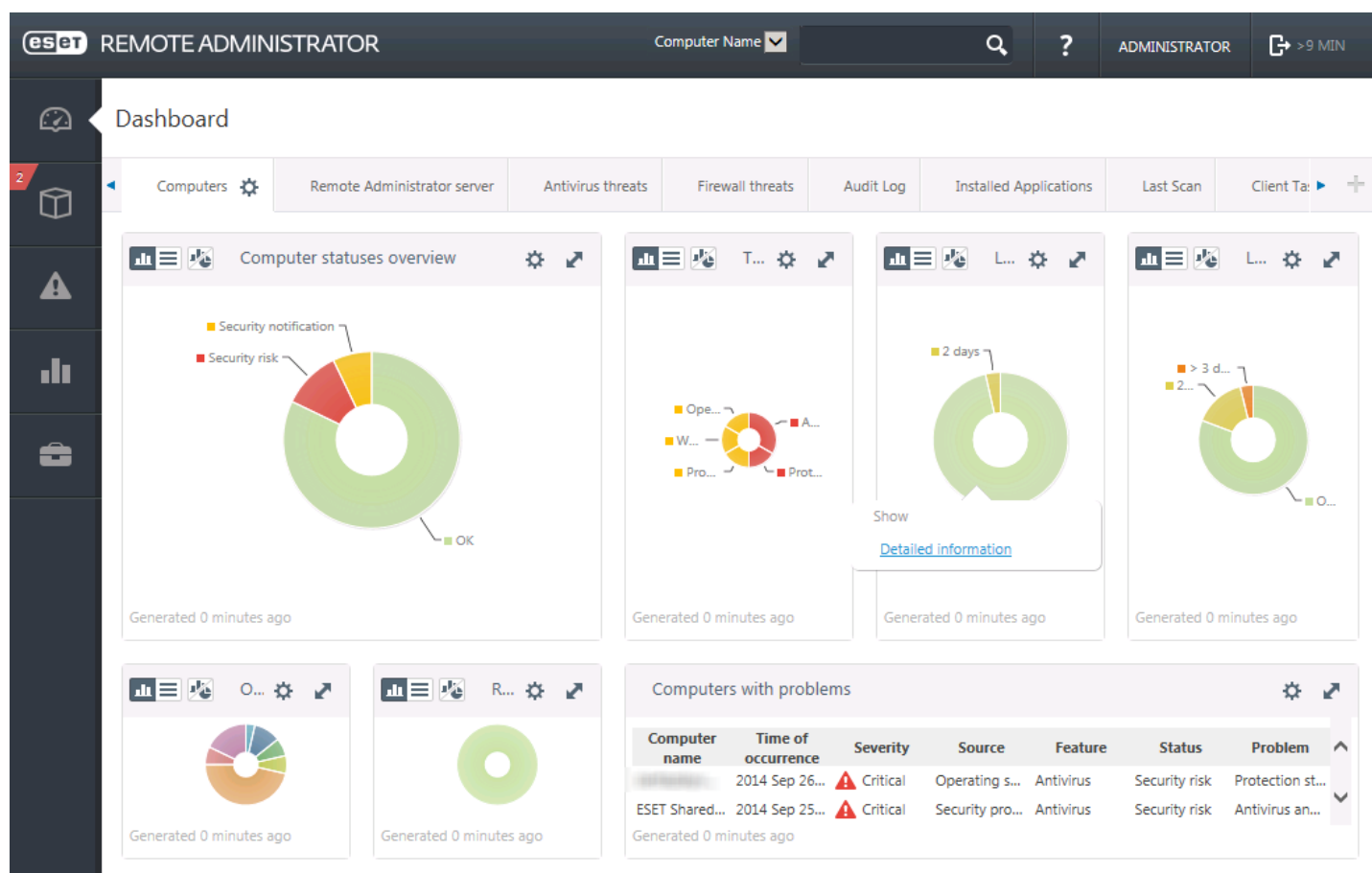
2.1 ESET Remote Administrator Server

ESET Remote Administrator Server é o componente executivo do ESET Remote Administrator. Ele processa todos os dados recebidos de clientes que se conectam ao Servidor (por meio do Agente ERA). O Agente ERA facilita a comunicação entre o cliente e o servidor. Dados (relatórios de cliente, configuração, replicação do agente, etc.) são armazenados em um banco de dados que o ERA acessa para fornecer relatórios.

Para processar dados corretamente, o Servidor ERA exige uma conexão estável com um servidor de banco de dados. Recomendamos que você instale o Servidor ERA e seu banco de dados em servidores separados para otimizar o desempenho. A máquina na qual o Servidor ERA está instalado deve ser configurada para aceitar todas as conexões de Agente/Proxy/RD Sensor, que são verificadas usando certificados. Uma vez que o Servidor ERA está instalado, é possível abrir o Console da Web ERA que permite gerenciar as estações de trabalho do endpoint com soluções ESET instaladas.

2.2 Console da Web

O **console da Web ERA** é uma interface de usuário na Web que apresenta dados do Servidor ERA e permite que você gerencie as soluções de segurança da ESET em seu ambiente. O Console da Web pode ser acessado usando um navegador. Ele exibe uma visão geral do status de clientes em sua rede e pode ser usado para implantar remotamente soluções da ESET em computadores não gerenciados. Você pode escolher tornar o servidor Web acessível pela internet, para permitir o uso do ESET Remote Administrator de praticamente qualquer lugar ou dispositivo.

O Painel do Console da Web:

A ferramenta **Pesquisa rápida** está localizada na parte superior do console da Web. Selecione **Nome do computador**, **Endereço IPv4/IPv6** ou **Nome da ameaça** no menu suspenso, digite sua sequência de pesquisa no campo de texto e clique no símbolo da lente de aumento ou pressione **Enter** para pesquisar. Você será redirecionado para a seção **Grupos**, onde seu resultado de pesquisa será exibido.

2.3 Proxy

Proxy ERA é outro componente do ESET Remote Administrator com duas finalidades principais. No caso de uma rede de médio porte ou corporativa com muitos clientes (por exemplo, 10.000 clientes ou mais), você pode usar o Proxy ERA para distribuir a carga entre vários Proxies ERA, facilitando para o Servidor ERA principal. A outra vantagem do Proxy ERA é que você pode usá-lo ao se conectar a uma filial remota com um link fraco. Isso significa que o Agente ERA em cada cliente não está conectando ao Servidor ERA principal diretamente através do Proxy ERA, que está na mesma rede local da filial. Esta configuração libera o link da filial. O Proxy ERA aceita conexões de todos os Agentes ERA locais, compila seus dados e os envia para o Servidor ERA principal (ou outro Proxy ERA). Isso permite que sua rede acomode mais clientes sem comprometer o desempenho de suas consultas de banco de dados e rede.

Dependendo da configuração de sua rede, é possível que um Proxy ERA se conecte a outro Proxy ERA e então se conecte ao Servidor ERA principal.

Para o funcionamento correto do Proxy ERA, o computador host no qual você instalará o Proxy ERA deverá ter um Agente da ESET instalado e deve estar conectado ao nível superior (seja Servidor ERA ou Proxy ERA superior, se houver um) de sua rede.

2.4 Agente

O **Agente ERA** é uma parte essencial do produto ESET Remote Administrator. As soluções de segurança ESET nas máquinas dos clientes (por exemplo ESET Endpoint Security) comunicam-se com o Servidor ERA exclusivamente por meio do Agente. Esta comunicação permite o gerenciamento das soluções de segurança ESET em todos os clientes remotos a partir de um local central. O Agente coleta informações do cliente e as envia para o Servidor. Quando o Servidor envia uma tarefa para o cliente, ela é enviada para o Agente, que então comunica-se com o cliente. Toda a comunicação em rede ocorre entre o Agente e a parte superior da rede do ERA: Servidor e Proxy.

O Agente ESET usa um dos seguintes três métodos para se conectar ao Servidor:

1. O Agente do Cliente é diretamente conectado ao Servidor.
2. O Agente do Cliente se conecta através de um Proxy, que é conectado ao Servidor.
3. O Agente do Cliente é conectado ao Servidor através de vários Proxies.

O Agente ERA comunica-se com soluções da ESET instaladas em um cliente, coleta informações de programas nesse cliente e transmite as informações de configuração recebidas do Servidor para o cliente.

OBSERVAÇÃO: O proxy da ESET tem seu próprio Agente, que processa todas as tarefas de comunicação entre clientes, outros proxies e o Servidor ERA.

2.5 Sensor RD

Sensor RD (Rogue Detection) é parte do ESET Remote Administrator desenvolvido para encontrar computadores na sua rede. O Sensor RD oferece uma forma conveniente de adicionar novos computadores ao ESET Remote Administrator sem a necessidade de encontrá-los e adicioná-los manualmente. Todo computador detectado em sua rede é exibido no console da Web e é adicionado por padrão ao grupo Todos. A partir daí, é possível realizar ações adicionais com computadores cliente individuais.

O Sensor RD consiste em um mecanismo de escuta passivo que detecta computadores que estão presentes na rede e envia informações sobre eles para o Servidor ERA. O Servidor ERA avalia se os PCs detectados na rede são desconhecidos ou se já são gerenciados.

3. Instalação remota

A instalação remota do ESET Endpoint Security a partir do ERA requer o seguinte:

- Instalação do Conector de dispositivo móvel
- Inscrição de dispositivos móveis

A instalação do ESET Endpoint Security em si pode ser feita de duas formas:

1. O Administrador envia o link de inscrição do aplicativo para os usuários finais via email junto com o arquivo de instalação APK e uma breve explicação sobre como instalá-lo. Ao tocar no link, os usuários são redirecionados para o navegador de Internet padrão do seu dispositivo Android e o ESET Endpoint Security será inscrito e conectado ao ERA. Se o ESET Endpoint Security não estiver instalado no dispositivo, ele será automaticamente redirecionado para a loja do Google Play para fazer download do aplicativo. Depois disso, uma instalação padrão será executada.
2. O Administrador envia o arquivo de configurações do aplicativo para os usuários finais via email junto com o arquivo de instalação APK e uma breve explicação sobre como instalá-lo. Alternativamente, os usuários serão solicitados a fazer download o arquivo APK a partir da loja do Google Play - o admin fornece o link. Depois da instalação, os usuários abrem o arquivo de configurações do aplicativo. Todas as configurações serão importadas e o aplicativo será ativado (desde que as informações de licença tenham sido incluídas).

4. Instalação local no dispositivo

O ESET Endpoint Security oferece aos administradores uma opção para configurar e gerenciar o Endpoint localmente, se eles optarem por não usar o ESET Remote Administrator. Todas as configurações do aplicativo são protegidas pela senha do administrador para que o aplicativo esteja totalmente sob o controle da administração em todos os momentos.

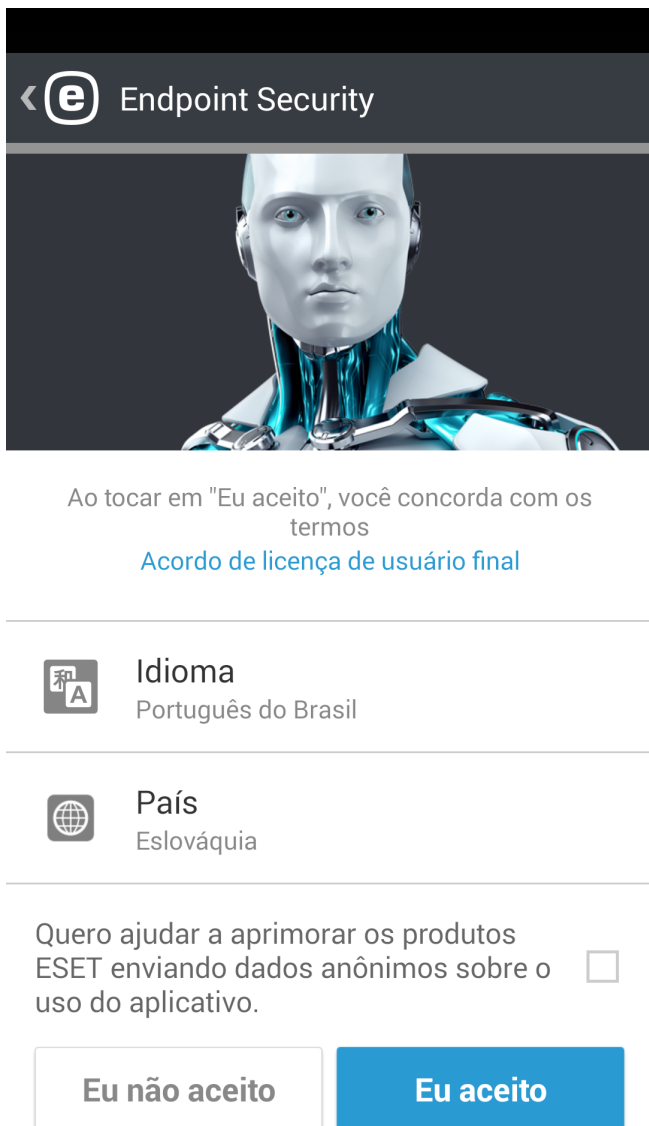
Se o administrador de uma pequena empresa decidir não usar o ESET Remote Administrator, mas ainda quer proteger os dispositivos corporativos e aplicar políticas de segurança básicas, ele tem duas opções sobre como gerenciar os dispositivos localmente:

1. Acesso físico a cada dispositivo da empresa e uma configuração manual das configurações.
2. O administrador pode preparar configuração desejada em seu dispositivo Android (com o ESET Endpoint Security instalado) e exportar essas configurações para um arquivo - veja a seção Importar/exportar configurações deste guia para mais informações). O administrador pode compartilhar o arquivo exportado com os usuários finais (por exemplo, via email) - eles podem importar o arquivo para qualquer dispositivo executando o ESET Endpoint Security. Quando o usuário abre e aceita o arquivo de configurações recebido, ele importará automaticamente todas as configurações e ativará o aplicativo (desde que as informações de licença tenham sido incluídas). Todas as configurações serão protegidas por uma senha de administrador.

4.1 Download do site da ESET

Faça o download do ESET Endpoint Security ao escanear o código QR abaixo usando seu dispositivo móvel e um aplicativo de leitura de QR:

Alternativamente, é possível fazer download do arquivo de instalação APK do ESET Endpoint Security do site da ESET:

1. Faça download do arquivo de instalação a partir do site da ESET.
2. Abra o arquivo a partir da área de notificação do Android ou localize-o usando um aplicativo gerenciador de navegação de arquivos. O arquivo normalmente é guardado na pasta Download.
3. Certifique-se de que os aplicativos de Fontes desconhecidas são permitidos no seu dispositivo. Para isso, toque no ícone do iniciador na tela inicial do Android ou vá para **Início** > **Menu**. Toque em **Configurações** > **Segurança**. A opção **Fontes desconhecidas** deve ser permitida.
4. Depois de abrir o arquivo, toque em **Instalar**.

4.2 Download do Google Play

Abra o aplicativo do Google Play Store no seu dispositivo Android e faça uma busca por ESET Endpoint Security (ou apenas ESET).

Alternativamente, é possível fazer download do programa ao escanear o código QR abaixo usando seu dispositivo móvel e um aplicativo de leitura de QR:

4.3 Assistente inicial

Quando o aplicativo estiver instalado, toque em **Configuração do administrador** e siga os avisos do assistente inicial. Este procedimento é destinado apenas para administradores:

1. Selecione o **idioma** que você deseja usar no ESET Endpoint Security.
2. Selecione o **país** onde trabalha ou reside atualmente.
3. Se desejar ajudar a aprimorar os produtos ESET enviando dados anônimos sobre o uso do aplicativo, selecione a opção apropriada.
4. Toque em **Eu aceito**. Ao fazer isso você concorda com o Contrato de Licença de Usuário Final.
5. Escolha se deseja conectar o ESET Endpoint Security ao ESET Remote Administrator ou realizar uma configuração manual. A última opção exigiria a criação de uma senha do administrador e ativar a proteção contra desinstalação.
6. Na próxima etapa, escolha se quer participar do ESET Live Grid. Para saber mais sobre o ESET Live Grid, consulte esta seção.
7. Selecione se você deseja que o ESET Endpoint Security detecte Aplicativos Potencialmente Indesejados. É possível encontrar mais detalhes sobre tais aplicativos nesta seção.
8. Ativar o produto.

5. Desinstalação

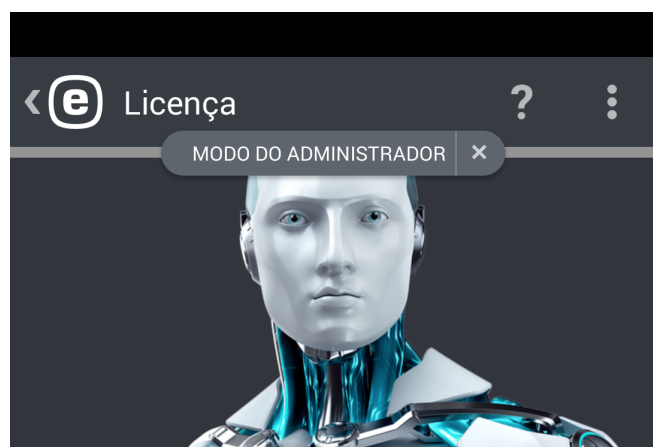
O ESET Endpoint Security pode ser desinstalado usando o assistente de desinstalação disponível no menu principal do programa em **Configurações** > **Desinstalar**. Se a Proteção contra desinstalar estiver ativada, você precisará digitar sua senha do administrador.

Alternativamente, você pode desinstalar o produto manualmente, seguindo estas etapas:

1. Toque no ícone do iniciador na tela inicial do Android (ou vá para **Início** > **Menu**) e toque em **Configurações** > **Segurança** > **Administradores do dispositivo**. Desmarque o ESET Endpoint Security e toque em **Desativar**. Toque em **Desbloquear** e insira a Senha de administrador. Se você não tiver definido o ESET Endpoint Security como o Administrador do dispositivo, ignore esta etapa.
2. Volte para **Configurações** e toque em **Gerenciar aplicativos** > ESET Endpoint Security > **Desinstalar**.

6. Ativação do produto

Há várias maneiras de ativar o ESET Endpoint Security. A disponibilidade de um método específico de ativação pode variar conforme o país, assim como os meios de distribuição (página da web da ESET, etc.) para seu produto.

Para ativar o ESET Endpoint Security diretamente no dispositivo Android, toque no ícone **Menu** na tela principal do ESET Endpoint Security (ou pressione o botão **MENU** em seu dispositivo) e toque em **Licença**.

OPÇÕES DE ATIVAÇÃO

Chave de licença
Ativar usando uma chave de licença

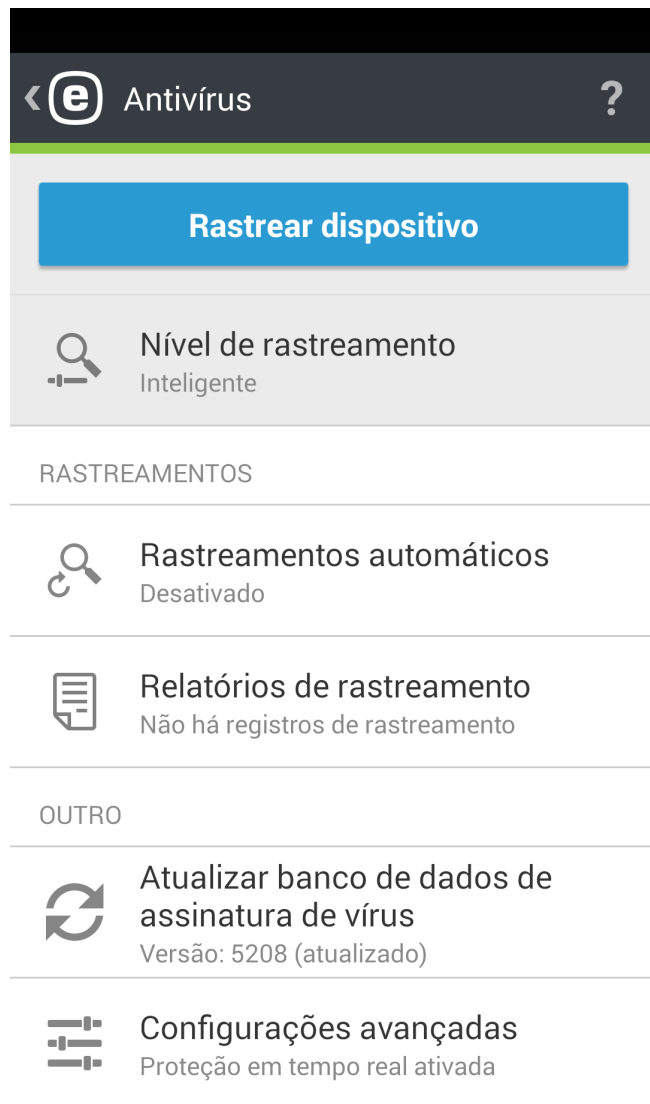
Conta de admin de segurança
Ative com uma licença da conta do Admin de segurança

Você pode usar qualquer um dos seguintes métodos para ativar o ESET Endpoint Security:

- **Chave de licença** - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usado para identificação do proprietário da licença e para ativação da licença.
- **Conta de admin de segurança**-Uma conta criada no portal do ESET License Administrator com credenciais (endereço de email e senha). Esse método permite que você gerencie várias licenças de um local.

OBSERVAÇÃO: ESET Remote Administrator é capaz de ativar dispositivos do cliente em segundo plano usando licenças disponibilizadas pelo administrador.

7. Antivírus

O módulo Antivírus protege seu dispositivo contra códigos maliciosos ao bloquear as ameaças e depois limpando ou movendo tais ameaças para a quarentena.

Rastrear dispositivo

Rastrear dispositivo pode ser usado para verificar se há infiltrações no dispositivo.

Alguns tipos de arquivo predefinidos são rastreados por padrão. Um rastreamento completo do dispositivo verifica a memória, os processos em execução e as bibliotecas de links dependentes, assim como os arquivos que fazem parte dos armazenamentos interno e removível. Um breve resumo do rastreamento será salvo em um arquivo de relatório disponível na seção Relatórios de rastreamento.

Para anular o rastreamento já em andamento, toque no ícone ☒.

Nível de Rastreamento

Há dois níveis diferentes de rastreamento para escolher:

- **Inteligente** - O rastreamento inteligente vai rastrear aplicativos instalados, arquivos DEX (arquivos executáveis para o sistema operacional Android), arquivos SO (bibliotecas) e arquivos ZIP com uma profundidade máxima de rastreamento de 3 arquivos aninhados e conteúdo de cartão de SD.
- **Profunda** - todos os tipos de arquivos, independentemente de sua extensão, serão verificados tanto na memória interna quanto no cartão SD.

Rastreamentos automáticos

Além do Rastreamento do dispositivo sob demanda, o ESET Endpoint Security também oferece rastreamentos automáticos. Para aprender a usar o Rastreamento no carregador e o Rastreamento Programado, leia esta seção.

Relatórios de rastreamento

Os relatórios de rastreamento contém dados abrangentes sobre rastreamentos completos na forma de arquivos de relatório. Consulte a seção Relatórios de rastreamento do antivírus deste documento para obter mais informações.

Atualizar banco de dados de assinatura de vírus

Por padrão, o ESET Endpoint Security inclui uma tarefa de atualização a fim de garantir que o programa seja atualizado regularmente. Para executar a atualização manualmente, toque em **Atualizar banco de dados de assinatura de vírus**.

OBSERVAÇÃO: Para evitar a utilização desnecessária da largura de banda, as atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça. Embora as atualizações sejam fornecidas gratuitamente com sua licença ativa, a operadora poderá cobrar pela transferência de dados.

As descrições detalhadas das Configurações Avançadas de Antivírus podem ser encontradas na seção Configurações Avançadas deste documento.

7.1 Rastreamentos automáticos

Nível de Rastreamento

Há dois níveis diferentes de rastreamento para escolher. Esta configuração é aplicável ao Rastreamento no carregador e Rastreamento Programado:

- **Inteligente** - O rastreamento inteligente vai rastrear aplicativos instalados, arquivos DEX (arquivos executáveis para o sistema operacional Android), arquivos SO (bibliotecas) e arquivos ZIP com uma profundidade máxima de rastreamento de 3 arquivos aninhados e conteúdo de cartão de SD.
- **Profunda** - todos os tipos de arquivos, independentemente de sua extensão, serão verificados tanto na memória interna quanto no cartão SD.

Rastreamento no carregador

Quando isto estiver selecionado, um rastreamento será iniciado automaticamente quando o dispositivo estiver no estado ocioso (totalmente carregado e conectado a um carregador).

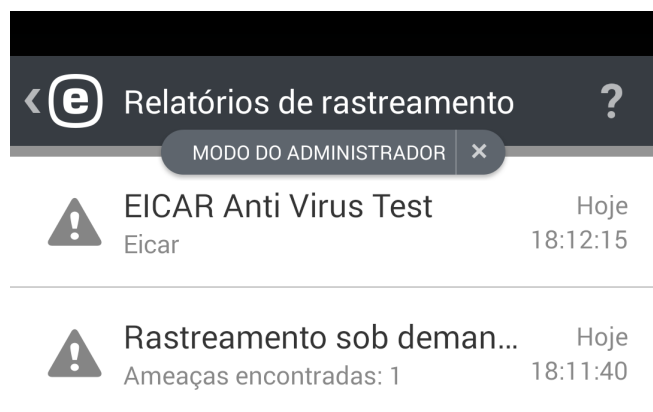
Rastreamento Programado

O rastreamento programado permite que você execute o rastreamento de Dispositivo automaticamente, em um horário predefinido. Para agendar um rastreamento, toque em ao lado de **Rastreamento programado** e especifique as datas e horários para que o rastreamento seja iniciado. Por padrão, está selecionado segunda-feira 04:00.

7.2 Relatórios de rastreamento

Relatórios de rastreamento são criados após cada rastreamento programado ou rastreamento de dispositivo acionado manualmente.

Cada relatório contém:

- data e hora do evento
- duração do rastreamento
- número de arquivos rastreados
- resultado do rastreamento ou erros ocorridos durante o rastreamento

7.3 Configurações avançadas

Proteção em tempo real

Esta opção permite que você ative/desative o rastreamento em tempo real. Este rastreamento é iniciado automaticamente na inicialização do sistema e rastreia os arquivos com os quais você interage. Ele rastreia automaticamente a pasta de Download, arquivos de instalação APK e todos os arquivos no cartão SD depois dele ser montado.

ESET Live Grid

Criado a partir do sistema de alerta antecipado avançado ThreatSense.NET, o ESET Live Grid foi projetado para fornecer níveis adicionais de segurança a seu dispositivo. Ele monitora constantemente os programas em execução no sistema e processa com relação à inteligência mais recente coletada de milhões de usuários do ESET em todo o mundo. Além disso, os rastreamentos são processados com mais rapidez e precisão conforme o banco de dados do ESET Live Grid cresce ao longo do tempo. Isso nos permite oferecer proteção proativa e velocidade de rastreamento melhores para todos os usuários ESET. Recomendamos que você ative este recurso. Obrigado pelo seu apoio.

Detectar Aplicativos Potencialmente Indesejados

Um aplicativo indesejado é um programa que contém adware, instala barras de ferramentas, rastreia seus resultados de pesquisa ou tem outros objetivos pouco claros. Existem algumas situações em que você pode sentir que os benefícios do aplicativo indesejado superam os riscos. Por isso a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso.

Detectar Aplicativos Potencialmente Inseguros

Há muitos aplicativos legítimos que têm a função de simplificar a administração dos dispositivos conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. A opção Detectar aplicativos potencialmente inseguros permite monitorar esses tipos de aplicativos e bloqueá-los, se você preferir. *Aplicativos potencialmente inseguros* é a classificação usada para software comercial legítimo. Essa classificação inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado.

Bloquear ameaças não solucionadas

Esta configuração determina uma ação padrão que será realizada após o rastreamento ser concluído e as ameaças serem encontradas. Se você ativar esta opção, o arquivo infectado não será executável.

Atualizações do banco de dados de assinatura de vírus

Esta opção permite que definir o intervalo de tempo para o download automático das atualizações do banco de dados de ameaças. Essas atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça ao banco de dados. Recomendamos que você deixe essa configuração no valor padrão (diariamente).

Idade máxima personalizada do banco de dados

Por padrão, o ESET Endpoint Security substitui o banco de dados de assinatura de vírus a cada 7 dias, mesmo se nenhuma atualização for emitida.

Servidor de atualização

Usando esta opção, você pode escolher atualizar seu dispositivo a partir do **servidor de pré-lançamento**. Atualizações em modo de teste são atualizações que passaram por testes internos e estarão disponíveis ao público geral em breve. Ao ativar as atualizações em modo de teste você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o modo de teste pode não ser sempre estável. A lista dos módulos atuais pode ser encontrada na seção **Sobre**: toque no ícone Menu ⋮ na tela principal do ESET Endpoint Security e toque em **Sobre** > ESET Endpoint Security. Se o usuário tiver apenas conhecimentos básicos, é recomendando deixar a opção **Servidor de lançamento** selecionada por padrão.

O ESET Endpoint Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outros dispositivos na rede. Uso de uma **Imagem local** - uma cópia dos arquivos de atualização no ambiente de rede local é conveniente, pois os arquivos de atualização não precisam ser obtidos por download a partir do servidor de atualização do fabricante repetidamente e por cada dispositivo móvel. Informações detalhadas sobre como configurar o servidor de imagem usando os produtos ESET Endpoint para Windows podem ser encontradas neste documento.

8. Antifurto

A funcionalidade **Antifurto** protege seu dispositivo móvel contra o acesso não autorizado.

Se você perder seu aparelho ou alguém roubá-lo e substituir seu cartão SIM por um cartão novo (não confiável), o dispositivo será bloqueado automaticamente pelo ESET Endpoint Security e um SMS de alerta será enviado para o(s) número(s) de telefone definido(s) pelo usuário. Essa mensagem incluirá o número de telefone do cartão SIM inserido no momento, o número IMSI (International Mobile Subscriber Identity, identidade internacional de assinante móvel) e o número IMEI (International Mobile Equipment Identity, identidade internacional de equipamento móvel) do telefone. O usuário não autorizado não terá conhecimento do envio desta mensagem porque ela será automaticamente excluída das sequências de mensagens do seu aparelho. Você também pode solicitar coordenadas de GPS do aparelho perdido ou apagar remotamente todos os dados armazenados no dispositivo.

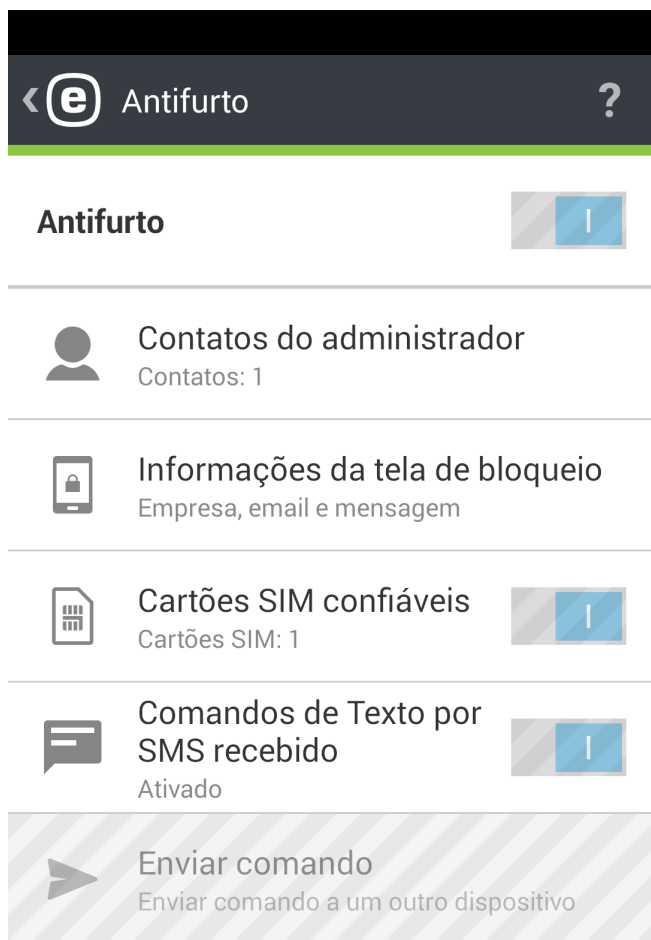
OBSERVAÇÃO: Certos recursos do Antifurto (Cartões SIM confiáveis e Comandos de Texto por SMS) não estão disponíveis em tablets que não tem suporte para mensagens.

Os recursos do Antifurto ajudam os administradores a proteger e localizar um aparelho perdido. As ações podem ser acionadas a partir do ERA ou por comandos de SMS.

O ESET Endpoint Security 2 usa os mesmos comandos SMS da versão 1 (Bloquear, Limpar e Encontrar). Os comandos a seguir, completamente novos, foram adicionados:

- **Desbloquear**-desbloqueia o aplicativo bloqueado
- **Redefinição de fábrica melhorada** - Todos os dados acessíveis no dispositivo serão removidos rapidamente (cabeçalhos de arquivos serão destruídos) e o dispositivo será redefinido para suas configurações padrão de fábrica.
- **Alarme** -o dispositivo perdido será bloqueado e reproduzirá um som muito alto mesmo se o dispositivo estiver no silencioso

Para fortalecer a segurança de comandos SMS, o administrador receberá um código de verificação SMS único e com tempo limitado em seu celular (no número definido na lista de contatos do Administrador) quando executar um comando SMS. Este código de verificação será usado para verificar um comando em particular.

Por exemplo, se um administrador envia um SMS para um dispositivo gerenciado (por exemplo, um telefone celular perdido) com o texto *eset lock,* ele vai receber um SMS com um código de verificação para esse comando. O administrador então envia um novo SMS para o mesmo número de telefone com o texto *eset lock* seguido do código de confirmação. Depois dessas etapas, o comando será verificado e executado. Comandos SMS podem ser enviados a partir de qualquer telefone celular e de qualquer número de celular listado nos contatos do administrador.

Ao executar comandos via SMS, o administrador recebe um SMS de confirmação de que um determinado comando foi enviado. Ao executar comandos ERA, o administrador recebe uma confirmação no ERA.

Ao receber informações de localização (comando Encontrar), o administrador usando o ESET Remote Administrator recebe as informações de localização na forma de coordenadas GPS. Ao executar o comando via SMS, as informações de localização (coordenadas de GPS e um link para o Google Maps) são recebidas via SMS. Ao usar a interface gráfica do usuário para os comandos de SMS (o recurso do **comando Enviar**), a informação recebida é apresentada na interface gráfica do usuário dedicada.

Todos os comandos do Antifurto podem ser realizados também a partir do ERA. Nova funcionalidade de gerenciamento de dispositivos móveis permite que os administradores executem os comandos Antifurto com apenas alguns cliques. As tarefas são imediatamente enviadas para execuções através de um novo componente de processamento de comandos push (Conector de dispositivo móvel), que agora é parte da infraestrutura do ERA.

8.1 Contatos do administrador

Esta é a lista de números de telefone do administrador protegidos pela senha do administrador. Comandos Antifurto só podem ser enviados de números confiáveis. Estes números também são usados para notificações relativas a ações Antifurto.

8.1.1 Como adicionar contato do Administrador

Um nome do administrador e número de telefone deve ser inserido durante o assistente de início do Antifurto. Caso o contato tenha mais de um número de telefone, todos os números associados serão considerados.

Os contatos do administrador podem ser adicionados ou modificados na seção **Antifurto** > **Contatos do administrador**.

8.2 Informações da tela de bloqueio

O administrador pode definir informações personalizadas (nome da empresa, endereço de email, mensagem) que serão exibidas quando o dispositivo for bloqueado, com a opção de ligar para um dos contatos do administrador pré-definidos.

Estas informações incluem:

- Nome da empresa (opcional)
- Endereço de email (opcional)
- Uma mensagem personalizada

8.3 Cartões SIM confiáveis

A seção **SIM Confiável** mostra a lista de cartões SIM confiáveis que serão aceitas pelo ESET Endpoint Security. Se você inserir um cartão SIM não definido nesta lista, a tela será bloqueada e um SMS de alerta será enviado para o administrador.

Para adicionar um novo cartão SIM, toque no ícone ➕. Digite um **Nome** para o Cartão SIM (por exemplo, casa, trabalho) e seu número IMSI (International Mobile Subscriber Identity). O IMSI (International Mobile Subscriber Identity) normalmente é apresentado como um número de 15 dígitos impresso no seu cartão SIM. Em alguns casos, ele pode ser mais curto.

Para remover um cartão SIM da lista, toque e segure a entrada e toque no ícone .

OBSERVAÇÃO: O recurso de SIM Confiável não está disponível em dispositivos CDMA, WCDMA e somente Wi-Fi.

8.4 Comandos remotos

Comandos remotos podem ser acionados de três maneiras:

- diretamente do Console ERA
- usando o recurso **Enviar comando** no ESET Endpoint Security instalado no dispositivo Android do administrador
- ao enviar mensagens de texto SMS do dispositivo do administrador

Para tornar a execução dos comandos SMS mais fácil para um administrador não usando o ERA, os comandos podem ser acionados a partir do ESET Endpoint Security instalado no dispositivo Android do administrador. Em vez de digitar manualmente a mensagem de texto e verificar o comando com o código de verificação, o administrador pode usar o recurso **Enviar comando** (disponível somente no modo Admin). Um Administrador pode digitar o número de telefone ou escolher um contato e selecionar o comando a ser enviado a partir do menu suspenso. O ESET Endpoint Security irá executar automaticamente todas as medidas necessárias silenciosamente em segundo plano.

Ao enviar comandos SMS, um número de telefone de administrador deve ser um Contato administrador no dispositivo de destino. O administrador receberá um código de verificação válido por uma hora, que pode ser usado para executar qualquer um dos comandos listados abaixo. O código deve ser anexado à mensagem na qual o comando é enviado com o seguinte formato: `eset find código`. O administrador receberá uma confirmação assim que o comando tiver sido executado no dispositivo de destino. Os comandos SMS a seguir podem ser enviados:

Localizar
Comando SMS: `eset find`
Você receberá uma mensagem de texto com as coordenadas de GPS do dispositivo de destino, incluindo um link para esse local no Google Maps. O dispositivo enviará uma nova SMS se um local mais preciso estiver disponível depois de 10 minutos.

Bloquear
Comando SMS: `eset lock`
Isto vai bloquear o dispositivo - será possível desbloquear usando a senha de admin ou o comando de desbloqueio. Ao enviar esse comando via SMS, você pode acrescentar uma mensagem personalizada que será exibida na tela do dispositivo bloqueado. Use o formato a seguir: `eset lock mensagem de código`. Se você deixar a mensagem de parâmetro vazia, uma mensagem da seção Informação tela de bloqueio será exibida.

Desbloquear
Comando SMS: `eset unlock`
O dispositivo será desbloqueado e o cartão SIM atualmente no dispositivo será salvo como SIM Confiável.

Tocar alarme
Comando SMS: `eset siren`
Um alarme alto vai começar a tocar mesmo se o dispositivo estiver configurado como silencioso.

Redefinição de fábrica melhorada
Comando SMS: `eset enhanced factory reset`
Isto vai redefinir o dispositivo para as configurações de fábrica. Todos os dados acessíveis serão apagados e os cabeçalhos de arquivos serão removidos. O processo pode demorar vários minutos.

Apagar
Comando SMS: `eset wipe`
Todos os contatos, mensagens, emails, contas, conteúdo do cartão SD, imagens, músicas e vídeos armazenados nas pastas padrão serão permanentemente apagados do dispositivo. O ESET Endpoint Security continuará instalado.

OBSERVAÇÃO: Os comandos SMS não diferenciam maiúsculas de minúsculas.

9. Controle de aplicativos

O recurso **Controle de aplicativos** oferece aos administradores a opção de monitorar os aplicativos instalados, bloquear o acesso a aplicativos definidos e diminuir o risco de exposição ao avisar os usuários para que desinstalem certos aplicativos. O administrador pode selecionar a partir de vários métodos de filtragem para aplicativos:

- Definir manualmente aplicativos que devem ser bloqueados
- Bloqueio com base em categoria (por exemplo, jogos ou social)
- Bloqueio baseado em permissões (por exemplo, aplicativos que rastreiam a localização)
- Bloquear por origem (por exemplo, aplicativos instalados com uma origem que não a loja do Google Play)

9.1 Regra de bloqueio

Na seção **Controle de Aplicativos** > **Bloqueio** > **Regras de bloqueio**, você pode criar regras de bloqueio do aplicativo com base nos seguintes critérios:

- nome do aplicativo ou nome do pacote
- categoria
- permissões

9.1.1 Bloqueio por nome do aplicativo

O ESET Endpoint Security dá aos administradores a opção de bloquear o aplicativo de acordo com o seu nome ou o nome do pacote. A seção **Regra de bloqueio** oferece um resumo das regras criadas e a lista de aplicativos bloqueados.

Para modificar uma regra existente, toque e segure a regra e toque em **Editar** . Para remover entradas de regras da lista, toque e segure uma das entradas, selecione as entradas que você deseja remover e toque em **Remover** . Para limpar a lista inteira, toque em **SELECIONAR TUDO** e depois em **Remover** .

Ao bloquear um aplicativo pelo nome, o ESET Endpoint Security irá procurar a correspondência exata com um nome de aplicativo lançado. Se você alterar a interface gráfica do usuário ESET Endpoint Security para um idioma diferente, é preciso reinserir o nome do aplicativo naquele idioma para ele continuar bloqueado.

Para evitar quaisquer problemas com nomes de aplicativos localizados, recomendamos bloquear tais aplicativos por seus nomes de pacotes - um identificador de aplicativo exclusivo que não pode ser alterado durante a execução ou reutilizado por outro aplicativo.

No caso de um administrador local, um usuário pode encontrar o nome do pacote de aplicativos em **Controle de aplicativos** > **Monitoramento** > **Aplicativos permitidos**. Depois de pressionar o aplicativo, a tela **Detalhes** exibirá o nome do pacote do aplicativo. Para bloquear o aplicativo, siga estes passos.

9.1.1.1 Como bloquear um aplicativo por seu nome

1. Toque em **Controle de aplicativos** > **Bloqueio** > **Bloquear aplicativo** > **Bloquear por nome**.
2. Escolha se deseja bloquear o aplicativo de acordo com o seu nome ou nome do pacote.
3. Digite as palavras com base em qual aplicativo será bloqueado. Para dividir várias palavras, use uma vírgula (,) como delimitador.

Por exemplo, a palavra "*poker*" no campo **Nome do aplicativo** vai bloquear todos os aplicativos que tiverem "*poker*" em seu nome. Se você digitar "*com.poker.game*" no campo **Nome do pacote**, o ESET Endpoint Security bloqueará apenas um aplicativo.

9.1.2 Bloqueio por categoria do aplicativo

O ESET Endpoint Security dá ao administrador a opção de bloquear o aplicativo de acordo com categorias de aplicativo pré-definidas. A seção **Regra de bloqueio** oferece um resumo das regras criadas e a lista de aplicativos bloqueados.

Se você quiser modificar uma regra existente, toque e segure a regra e toque em **Editar** .

Para remover algumas entradas de regras da lista, toque e segure uma das entradas, selecione as entradas que você deseja remover e toque em **Remover** . Para limpar a lista inteira, toque em **SELECIONAR TUDO**.

9.1.2.1 Como bloquear um aplicativo com base em sua categoria

1. Toque em **Controle de aplicativos** > **Bloqueio** > **Bloquear aplicativo** > **Bloquear por categoria**.
2. Selecione as categorias pré-definidas usando caixas de seleção e toque em **Bloquear**.

9.1.3 Bloqueio por permissões do aplicativo

O ESET Endpoint Security dá ao administrador a opção de bloquear o aplicativo de acordo com suas permissões. A seção **Regra de bloqueio** oferece um resumo das regras criadas e a lista de aplicativos bloqueados.

Se você quiser modificar uma regra existente, toque e segure a regra e toque em **Editar** .

Para remover algumas entradas de regras da lista, toque e segure uma das entradas, selecione as entradas que você deseja remover e toque em **Remover** . Para limpar a lista inteira, toque em **SELECIONAR TUDO**.

9.1.3.1 Como bloquear um aplicativo por suas permissões

1. Toque em **Controle de aplicativos** > **Bloqueio** > **Bloquear aplicativo** > **Bloquear por permissão**.
2. Selecione as permissões usando caixas de seleção e toque em **Bloquear**.

9.1.4 Bloquear fontes desconhecidas

Por padrão, o ESET Endpoint Security não bloqueia os aplicativos obtidos a partir da Internet ou de qualquer outra fonte que não a loja Google Play. A seção **Aplicativos bloqueados** fornece uma visão geral dos aplicativos bloqueados (nome do pacote, regra aplicada) e a opção de desinstalar o aplicativo ou adicioná-lo à lista de permissões - seção **Exceções**.

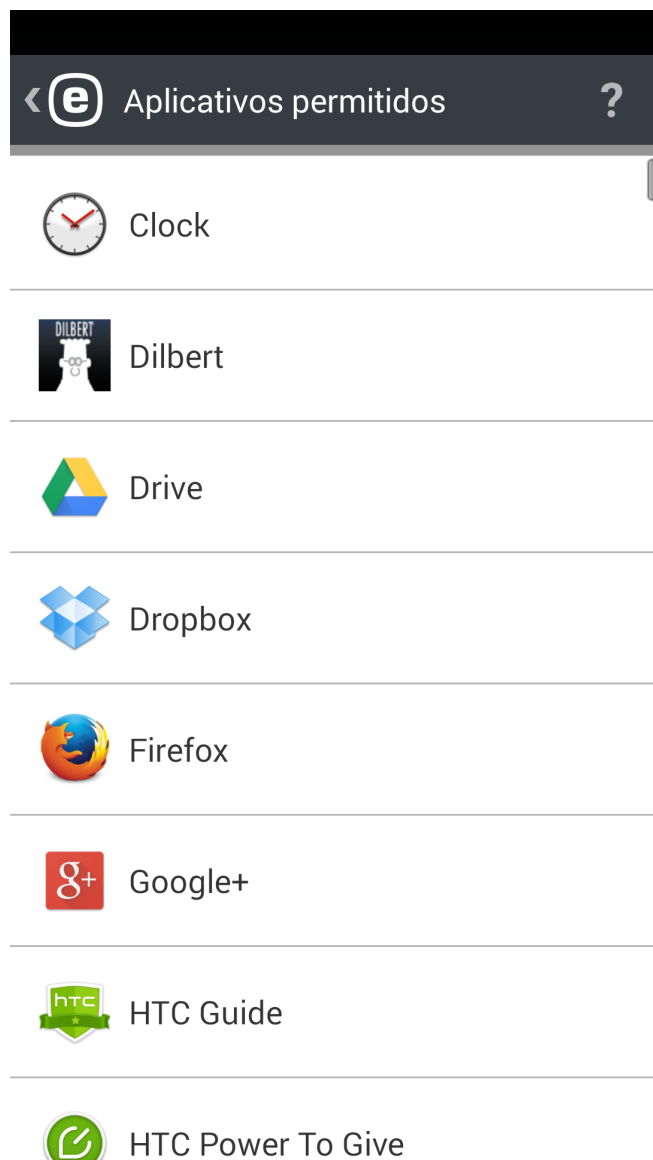
9.2 Exceções

Você pode criar exceções para excluir um aplicativo específico da lista de aplicativos bloqueados. Administradores gerenciando o ESET Endpoint Security remotamente podem usar este novo recurso para determinar se um determinado dispositivo está de acordo com a política da empresa em relação a aplicativos instalados.

9.2.1 Como adicionar exceções

Além de adicionar uma nova exceção (digitando o nome do pacote de aplicativos), os aplicativos também podem ser colocados na lista de permissões ao serem retirados da lista de **Aplicativos bloqueados**.

9.3 Aplicativos permitidos

Esta seção oferece um resumo de aplicativos instalados que não estão bloqueados por regras de bloqueio. Para bloquear qualquer aplicativo listado aqui, toque no aplicativo, toque no ícone **Menu** no canto superior direito da tela e toque em **Bloquear**. O aplicativo será movido para lista de **Aplicativos bloqueados** (em **Controle de aplicativos** > **Bloqueio**).

9.4 Permissões

Este recurso controla o comportamento das aplicativos com acesso a dados pessoais ou da empresa e permite que o administrador monitore o acesso do aplicativo com base em categorias de permissões pré-definidas.

Alguns aplicativos instalados no seu dispositivo podem ter acesso a serviços que cobram, rastreiam sua localização ou lêem suas informações de identidade, contatos ou mensagens de texto. O ESET Endpoint Security fornece uma auditoria para estes aplicativos.

Nesta seção, você pode ver a lista de aplicativos classificados por categoria. Toque em cada categoria para ver sua descrição detalhada. Os detalhes de permissões de cada aplicativo podem ser acessados tocando em um determinado aplicativo.

Permissões

Administrador do dispositivo
Aplicativos: 1

Usar serviços pagos
Aplicativos: 19

Rastrear localização
Aplicativos: 20

Ler informações identificadas
Aplicativos: 39

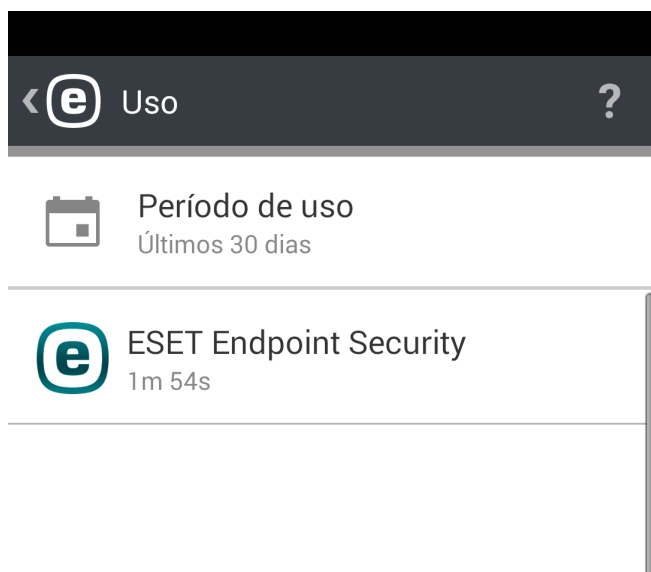
Ler dados pessoais
Aplicativos: 14

Mídia de registro
Aplicativos: 15

Acessar mensagens
Aplicativos: 15

Acessar contatos

9.5 Uso

Nesta seção, o administrador pode monitorar quanto tempo um usuário gasta em aplicativos específicos. Para filtrar a lista de aplicativos pelo seu período de uso, use a opção **Período de uso** e escolha se deseja exibir os aplicativos usados nos últimos 30 dias, 7 dias ou 24 horas.

10. Segurança do dispositivo

Segurança do dispositivo fornece aos administradores opções para realizar o seguinte:

- executa políticas básicas de segurança em de dispositivos móveis e define políticas para configurações importantes do dispositivo
- especifica a força requerida do bloqueio de tela
- uso da câmera embutida restrito

10.1 Política de bloqueio de tela

Nesta seção, o administrador é capaz de:

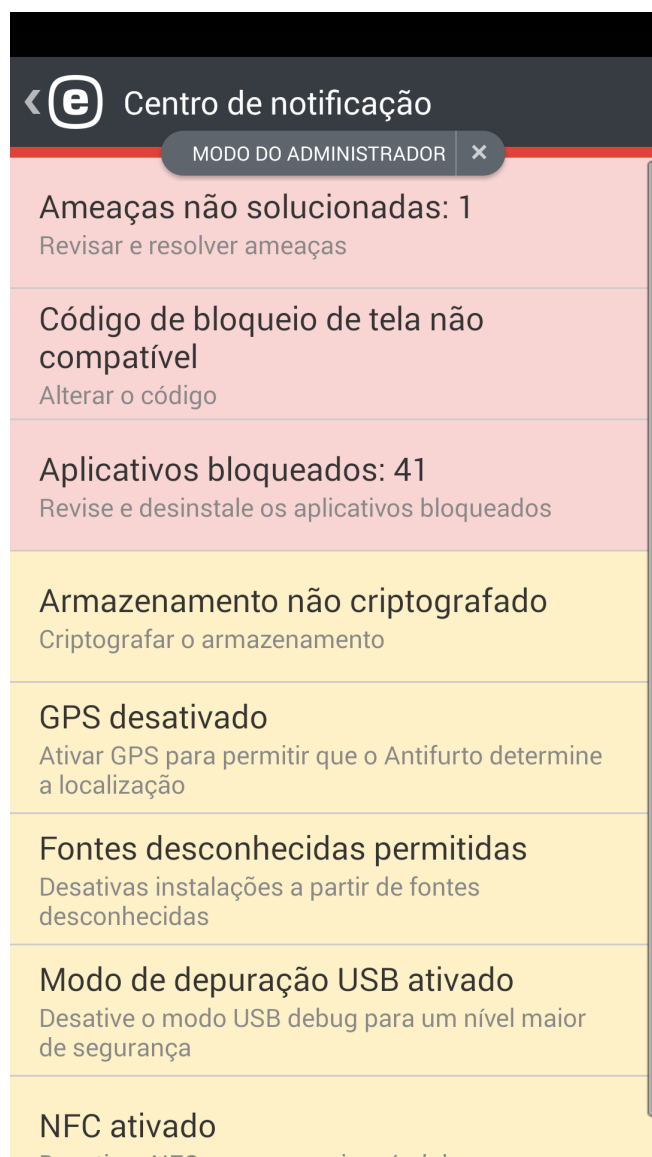
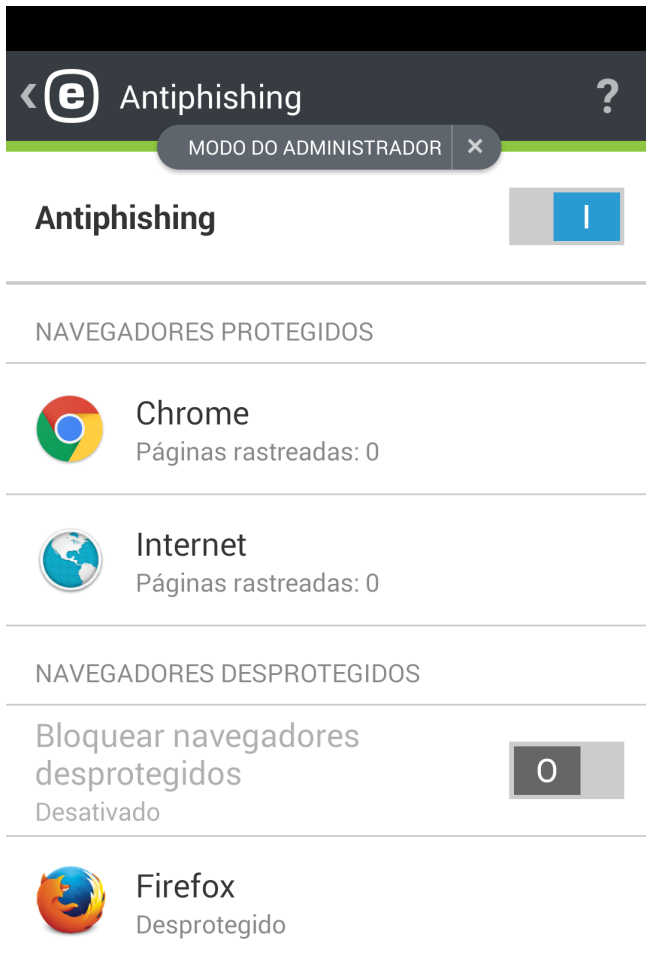
- definir um nível mínimo de segurança (padrão, PIN, senha) para o código de bloqueio da tela do sistema e definir a complexidade do código (por exemplo, comprimento mínimo do código)
- define o número máximo de tentativas falhas de desbloquear (ou o dispositivo irá para o padrão de fábrica)
- definir idade máxima do código de bloqueio de tela
- configurar o temporizador da tela de bloqueio

O ESET Endpoint Security notifica automaticamente o usuário e o administrador se as configurações atuais do dispositivo estiverem de acordo com as políticas de segurança corporativa. Se um dispositivo estiver fora de conformidade, o aplicativo irá automaticamente sugerir ao usuário o que deve ser alterado para estar em conformidade novamente.

10.2 Política de configurações de dispositivo

A Segurança do dispositivo também inclui sua **Política de configurações de dispositivo** (anteriormente, parte da funcionalidade da auditoria de segurança) que dá ao administrador do sistema a opção de monitorar as configurações pré-definidas do dispositivo para determinar se elas estão no estado recomendado.

Configurações de dispositivo incluem:

- Wi-Fi
- Satélites GPS
- Serviços de localização
- Memória
- Roaming de dados
- Roaming de chamada
- Fontes desconhecidas
- Modo de depuração
- NFC
- Criptografia de armazenamento
- Dispositivo com root

11. Antiphishing

O termo *roubo de identidade* define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, números de cartão de crédito, códigos de PIN ou nomes de usuário e senhas.

Recomendamos manter o **Antiphishing** ativado. Todos os potenciais ataques de phishing que vêm de sites ou domínios listados no banco de dados de malware da ESET serão bloqueados e uma notificação de alerta será exibida informando sobre o ataque.

O Antiphishing pode ser integrado com os navegadores mais comuns disponíveis no sistema operacional Android (por exemplo o Chrome e navegador padrão Android). Outros navegadores serão listados como desprotegidos e o acesso a eles pode ser bloqueado, clicando no botão O.

Para aproveitar ao máximo a funcionalidade do Antiphishing, recomendamos que você bloqueie todos os navegadores não compatíveis, de modo que os usuários só possam usar os navegadores compatíveis.

OBSERVAÇÃO: O Antiphishing não pode protegê-lo durante a navegação em modo privado (anônimo).

12. SMS e Filtro de Chamadas

O **SMS e Filtro de Chamadas** bloqueia mensagens SMS/MMS recebidas e chamadas recebidas/realizadas de acordo com as regras definidas pelo usuário.

Mensagens indesejadas geralmente incluem anúncios de operadoras ou mensagens de usuários desconhecidos ou indeterminados. O termo bloquear mensagens refere-se à transferência automática de uma mensagem recebida para a seção **Histórico**. Nenhuma notificação é exibida quando uma mensagem ou chamada recebida é bloqueada. A vantagem é que o usuário não é incomodado pelas informações indesejadas, mas, ao mesmo tempo, pode consultar os relatórios para procurar mensagens que possam ter sido bloqueadas por engano.

OBSERVAÇÃO: O SMS e Filtro de Chamadas não funciona em tablets que não suportam chamadas e mensagens. Filtros SMS/MMS não estão disponíveis para dispositivos Android OS 4.4 (KitKat), e serão desativados em dispositivos onde o Google Hangouts é definido como o principal aplicativo de SMS.

Para bloquear chamadas e mensagens vindas do último número de telefone recebido, toque em **Bloquear o Último que ligou** ou **Bloquear o Último a Enviar SMS**. Isto irá cria uma nova regra.

12.1 Regras

Como usuário, você pode criar regras de usuários sem precisar inserir a senha do administrador. Regras de Admin só podem ser criadas no modo Admin. Regras de administrador vão anular as regras do usuário.

Mais informações sobre a criação de uma nova regra podem ser encontradas nesta seção.

Se você quiser remover uma entrada de regra existente da lista de **Regras**, toque e segure na entrada e toque no ícone **Remover** .

12.1.1 Como adicionar uma nova regra

Para adicionar uma nova regra, toque no ícone ➕ no canto superior direito da tela **Regras**.

Com base na ação que você deseja que a regra execute, escolha se as mensagens e chamadas serão permitidas ou bloqueadas.

Especifique uma pessoa ou grupo de números de telefone. O ESET Endpoint Security reconhecerá os grupos de contato salvo em seus Contatos (por exemplo Família, Amigos ou Trabalho). **Todos os números desconhecidos** vai incluir os números de telefone que não estão salvos na sua lista de contatos. Você pode usar essa opção para bloquear chamadas indesejadas (por exemplo, ligações de telemarketing) ou para evitar que funcionários disquem números desconhecidos. A opção **Todos os números conhecidos** diz respeito a todos os números de telefone guardados na sua lista de contatos. **Números restritos** serão aplicados para ligações de pessoas que ocultaram seu número de telefone deliberadamente pelo recurso de restrição de identificação da linha chamadora.

Especifique o que deve ser bloqueado ou permitido:

- chamadas enviadas
- chamadas recebidas
- mensagens de texto (SMS) recebidas ou
- mensagens multimídia (MMS) recebidas

Para aplicar a regra apenas por um tempo determinado, toque em **Sempre** > **Personalizado** e selecione os dias da semana e um intervalo de tempo em que você quer que a regra seja aplicada. Por padrão, sábado e domingo estão selecionados. Esta funcionalidade pode vir a calhar se você não quiser ser incomodado durante reuniões, viagens de negócios, durante a noite ou o fim de semana.

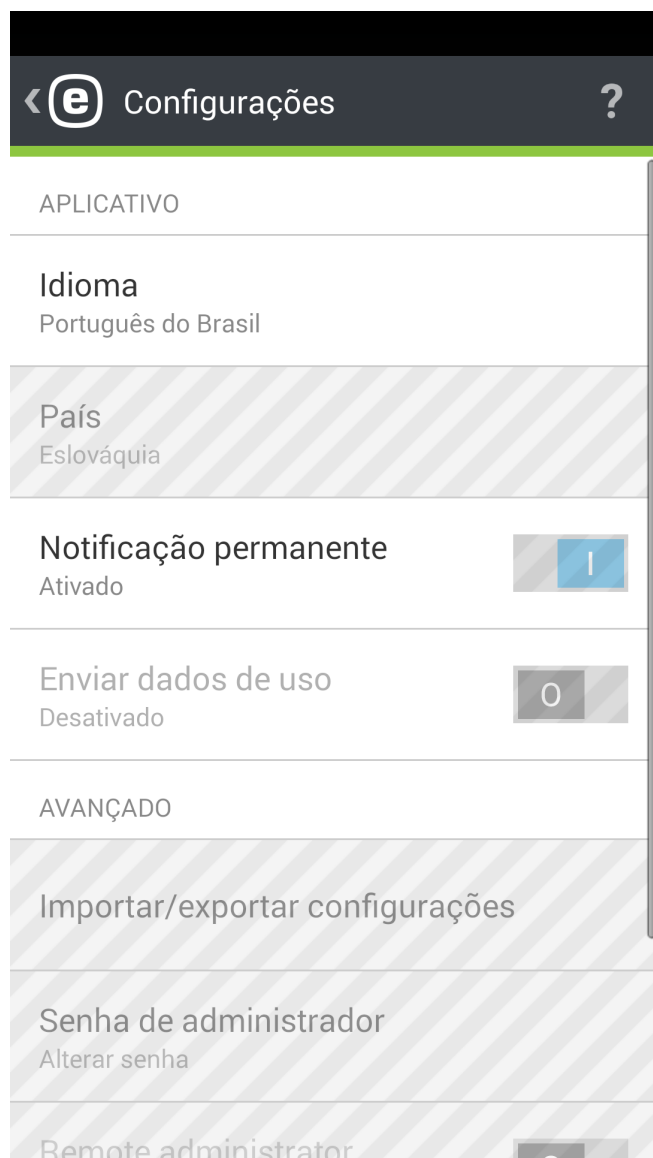
OBSERVAÇÃO: Se você estiver no exterior, todos os números de telefone inseridos na lista deve incluir o código de discagem internacional seguido pelo número propriamente dito (por exemplo, +1610100100).

12.2 Histórico

Na seção **Histórico** você pode consultar as chamadas e mensagens bloqueadas ou permitidas pelo SMS e Filtro de Chamadas. Cada relatório contém o nome do evento, o número de telefone correspondente e a data e a hora do evento. Os registros de mensagens SMS e MMS também preservam o corpo da mensagem.

Se você quiser modificar uma regra relacionada ao número de telefone ou contato que foi bloqueado, selecione a entrada na lista tocando nela e no ícone .

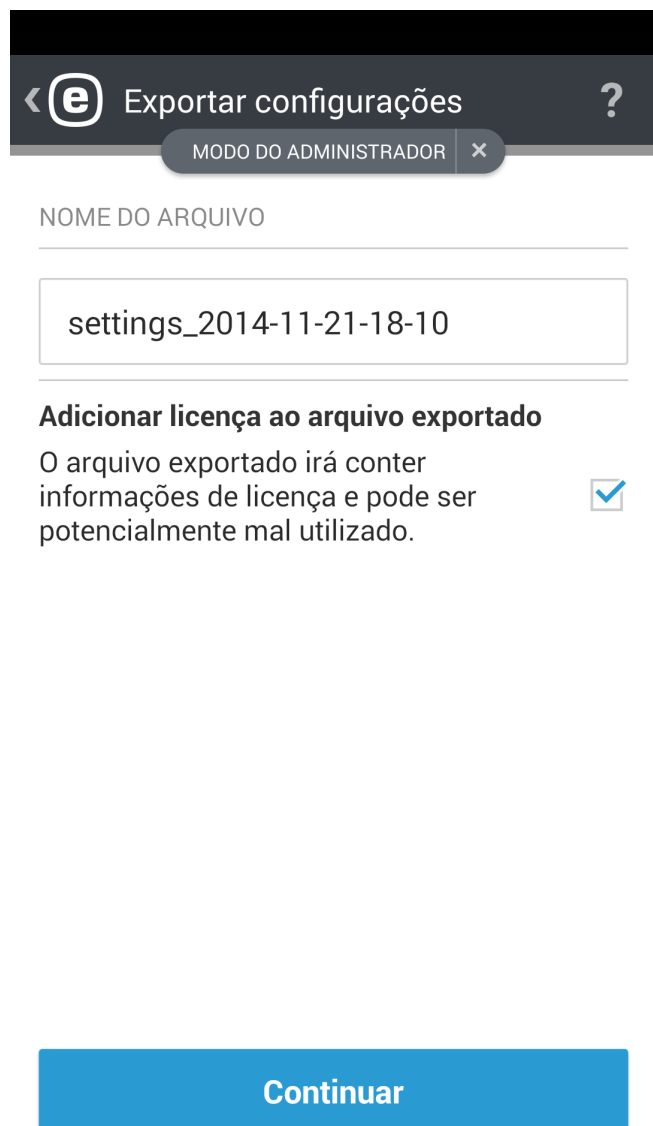
Para remover a entrada da lista, selecione-a e toque no ícone . Para remover mais entradas, toque e segure uma das entradas, selecione as entradas que você deseja remover e toque no ícone .

13. Configurações

Idioma
Por padrão, o ESET Endpoint Security é instalado no idioma definido em seu dispositivo como local do sistema (nas configurações de idioma e teclado do sistema operacional Android). Para alterar o idioma da interface de usuário do aplicativo, toque em Idioma e selecione o idioma desejado.

País
Selecione o país onde trabalha ou reside atualmente.

Atualizar
Para o máximo de proteção, é importante usar a versão mais recente do ESET Endpoint Security. Toque em **Atualizar** para ver se há uma nova versão disponível para download no site da ESET. Esta opção não está disponível se você fez o download do ESET Endpoint Security a partir do Google Play - neste caso, o produto é atualizado a partir do Google Play.

Notificação permanente
o ESET Endpoint Security exibe seu ícone de notificação no canto superior esquerdo da tela (barra de status do Android). Se você não deseja que esse ícone seja exibido, desmarque **Notificação permanente**.

Enviar dados de uso
Esta opção ajuda a melhorar os produtos ESET enviando dados anônimos sobre o uso do aplicativo. Se você não ativou esta opção durante o assistente de inicialização de instalação, é possível fazer isso na seção **Configurações**.

Senha de administrador
Esta opção permite que você defina uma nova senha de administrador ou altere a senha existente. Para saber mais, consulte a seção Senha de administrador deste documento.

Desinstalar
Ao executar o assistente de desinstalação, o ESET Endpoint Security e a pasta de quarentena serão removidos permanentemente do dispositivo. Se a Proteção contra desinstalar foi ativada, você precisará digitar a **senha do administrador**.

13.1 Importar/exportar configurações

Para compartilhar facilmente as configurações de um dispositivo móvel com outro se o dispositivo não for gerenciado pelo ERA, o ESET Endpoint Security 2 apresenta a opção de exportar e importar configurações do programa. O administrador pode exportar manualmente configurações do dispositivo para um arquivo que pode então ser compartilhado (por exemplo, via email) e importado para qualquer dispositivo executando o aplicativo do cliente. Quando o usuário aceita o arquivo de configurações recebido, ele define automaticamente todas as configurações e ativa o aplicativo (desde que as informações de licença tenham sido incluídas). Todas as configurações serão protegidas por uma senha de administrador.

13.1.1 Exportar configurações

Para exportar as configurações atuais do ESET Endpoint Security, especifique as configurações de nome de arquivo - a data e hora atual serão automaticamente preenchidos. Você também pode adicionar informações da licença (chave de licença ou endereço de email e senha da conta do administrador de segurança) para o arquivo exportado, mas cuidado, esta informação não será criptografada e pode ser mal utilizada.

Na etapa adicional, selecione a forma como você quer compartilhar o arquivo:

- Rede Wi-fi
- Bluetooth
- Email
- Gmail
- aplicativo de navegação de arquivo (por exemplo, ASTRO File Manager ou ES File Explorer)

13.1.2 Importar configurações

Para importar as configurações de um arquivo localizado no dispositivo, use um aplicativo de navegação de arquivos, como o ASTRO File Manager ou ES File Explorer, localize o arquivo de configurações e selecione ESET Endpoint Security.

As configurações também podem ser importadas ao selecionar um arquivo na seção **Histórico**.

13.1.3 Histórico

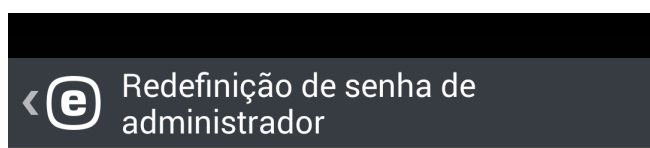
A seção **Histórico** oferece uma lista de arquivos de configuração importados e permite que você compartilhe, importe ou remova esses arquivos.

13.2 Senha de administrador

A **Senha de administrador** é necessária para desbloquear o dispositivo, enviar comandos do Antifurto, acessar recursos protegidos com senha e desinstalar o ESET Endpoint Security.

IMPORTANTE: Escolha a senha cuidadosamente. Para aumentar a segurança e fazer com que a senha seja mais difícil de adivinhar, use uma combinação de letras minúsculas, maiúsculas e números.

Para redefinir a senha do administrador em um dispositivo com uma tela bloqueada:

1. Toque em **Senha esquecida?** > **Continuar** > **Solicitar código de verificação**. Se o dispositivo não estiver conectado à Internet, toque no link **escolher redefinição off-line** e entre em contato com o Atendimento ao Cliente da ESET.
2. Verificar seu email - um email contendo o código de verificação e ID do dispositivo será enviado para o endereço de email associado à licença ESET. O código de verificação estará ativo por uma hora após seu recebimento.
3. Digite o código de verificação e a nova senha na tela bloqueada do seu dispositivo.

Redefinição de senha de administrador

Você está tentando redefinir a senha de administrador. Um email contendo o código de verificação e ID do dispositivo será enviado para seu email da licença.

Você realmente deseja redefinir a senha de administrador?

Anterior | Continuar

13.3 Remote administrator

O ESET Remote Administrator (ERA) permite gerenciar o ESET Endpoint Security em um ambiente de rede a partir de um local centralizado.

O uso do ERA não só aumenta seu nível de segurança, mas também facilita a administração de todos os produtos da ESETinstalados nos dispositivos móveis e estações de trabalho clientes. Dispositivos com o ESET Endpoint Security podem se conectar ao ERA usando qualquer tipo de conexão com a internet - WiFi, LAN, WLAN, rede celular (3G, 4G, HSDPA, GPRS), etc. - desde que seja uma conexão com a internet regular (sem um proxy ou firewall) e ambos os endpoints estejam configurados corretamente.

Ao se conectar ao ERA por uma rede celular, uma conexão bem-sucedida dependerá do provedor de rede móvel e exigirá uma conexão com a internet completa.

Para conectar um dispositivo ao ERA, adicione o dispositivo na lista de **Computadores** no Console da Web ERA, registre o dispositivo usando a tarefa de **Inscrição de Dispositivo** e digite o Mobile Device Connector (MDC) endereço do servidor:

- **Host do servidor** - especifica o nome DNS completo ou o endereço IP público do servidor executando o Mobile Device Connector (MDC). O nome de host só pode ser usado se você estiver se conectando através de uma rede Wi-Fi interna.
- **Porta do servidor** - permite especificar a porta de servidor utilizada para conexão ao Mobile Device Connector.

OBSERVAÇÃO: Saiba mais sobre como para gerenciar sua rede usando o ESET Remote Administrator, consulte a ESET Remote Administrator documentação on-line.

13.4 ID do dispositivo

O ID do dispositivo ajuda o administrador a identificar seu dispositivo caso ele seja perdido ou roubado.

14. Atendimento ao cliente

Os especialistas de atendimento ao cliente ESET estão disponíveis para ajudar caso você precise de assistência administrativa ou suporte técnico relacionado ao ESET Endpoint Security ou a qualquer outro produto ESET.

Para enviar uma solicitação de atendimento diretamente de seu dispositivo, toque no ícone do Menu na tela principal do ESET Endpoint Security (ou pressionando o botão MENU no seu dispositivo), toque em **Atendimento ao cliente** > **Atendimento ao Cliente** e preencha todos os campos obrigatórios.

Visite a Base de conhecimento da ESET para encontrar soluções rápidas para dúvidas comuns. Você também pode enviar uma pergunta através do formulário de Atendimento ao Cliente.

Atendimento ao cliente
Enviar solicitação de suporte

Base de conhecimento ESET
Apenas em inglês

o ESET Endpoint Security inclui recursos avançados de registro em relatório para ajudar a diagnosticar possíveis problemas técnicos. Para fornecer para a ESET um relatório detalhado do aplicativo, certifique-se de que **Enviar relatório do aplicativo** está selecionado (padrão). Toque em **Enviar** para enviar sua solicitação. Um Especialista de Atendimento ao Cliente ESET vai entrar em contato com você no endereço de email fornecido.